Laboratoire 3 - Configuration de la stratégie de sécurité locale de Windows

Introduction

Au cours de ce laboratoire vous configurerez l**a stratégie de sécurité locale de Windows**. La stratégie de sécurité locale de Windows permet de configurer de nombreux éléments de sécurité pour les ordinateurs autonomes.

IMPORTANT: Créez un nouveau document Word et enregistrez-le comme VotreNom_Lab3.docx. Il y aura des étapes où je vous demande de coller des captures d'écran dans ce document.

Étape 1 : Examinez les exigences en matière de sécurité.

Un client a besoin de six ordinateurs Windows autonomes dans une de ses filiales. Ils doivent être configurés conformément à la stratégie de sécurité de l'entreprise.

Les stratégies doivent être configurées manuellement sur chaque ordinateur.

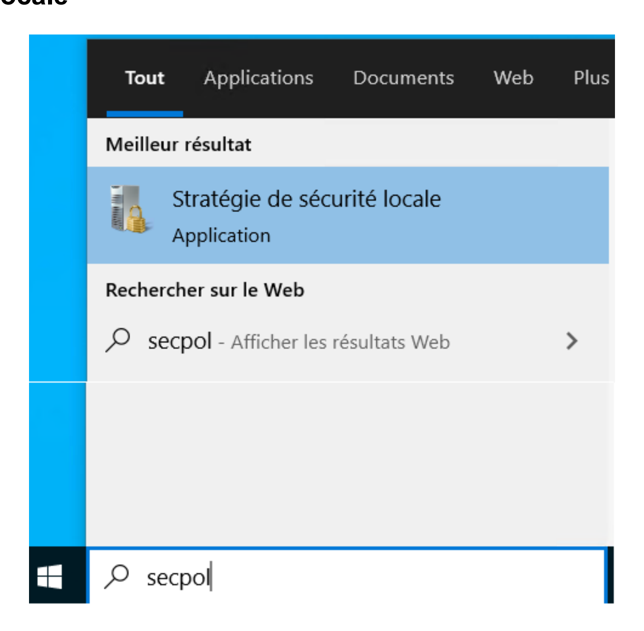
La stratégie de sécurité est la suivante :

- Les mots de passe doivent contenir au moins 8 caractères.
- Les mots de passe doivent être changés tous les 90 jours.
- Les utilisateurs peuvent changer de mot de passe une fois par jour.
- Les utilisateurs peuvent réutiliser un mot de passe unique après l'utilisation de 8 autres.
- Les mots de passe doivent comprendre trois des quatre éléments suivants :
  - Au moins un caractère alphanumérique en minuscules.
  - Au moins un caractère alphanumérique en majuscules.
  - Au moins un caractère numérique.
  - Au moins un symbole.
- Les utilisateurs ne peuvent plus accéder à leur ordinateur après 5 tentatives erronées de saisie du mot de passe. Les utilisateurs doivent patienter 5 minutes avant que le compteur se réinitialise et permette à nouveau de saisir un mot de passe.
- Le paramètre **Auditer les événements de connexion aux comptes** doit être activé.
- Après 30 minutes d'inactivité, l'utilisateur est automatiquement déconnecté.
- Les utilisateurs reçoivent un rappel les avertissant qu'ils doivent changer de mot de passe 7 jours avant son expiration.
- Lors de la connexion, le titre et le texte suivants doivent s'afficher :
  - Titre : Attention :
  - Texte : Votre activité est surveillée. Cet ordinateur est conçu pour une utilisation professionnelle uniquement.

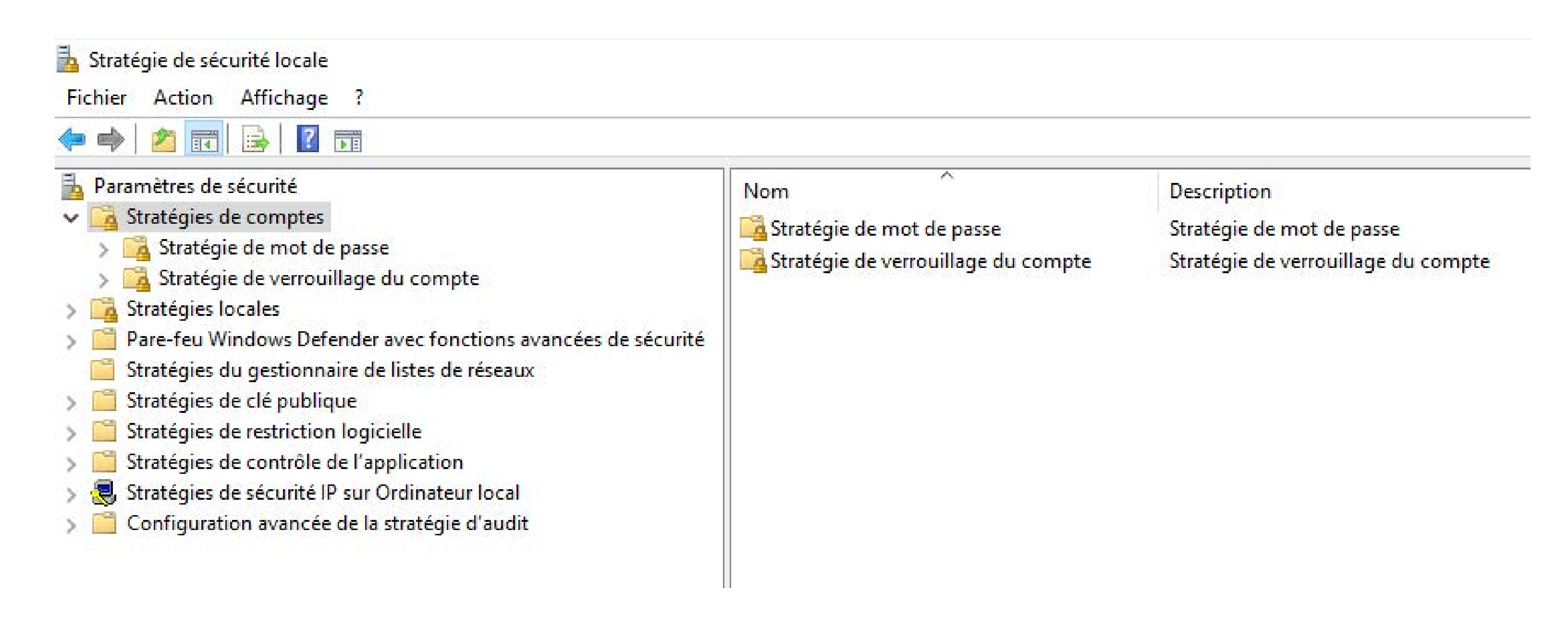
Étape 2 : Ouvrez l'outil Stratégie de sécurité locale de Windows.

a. Connectez-vous au VPN du collège et ouvrez une session sur votre machine virtuelle Windows 10 avec l'utilisateur **etudiantadmin.**

b. Pour accéder à la Stratégie de sécurité locale dans Windows 10, tapez: **secpol** puis cliquez sur **Stratégie de sécurité locale**



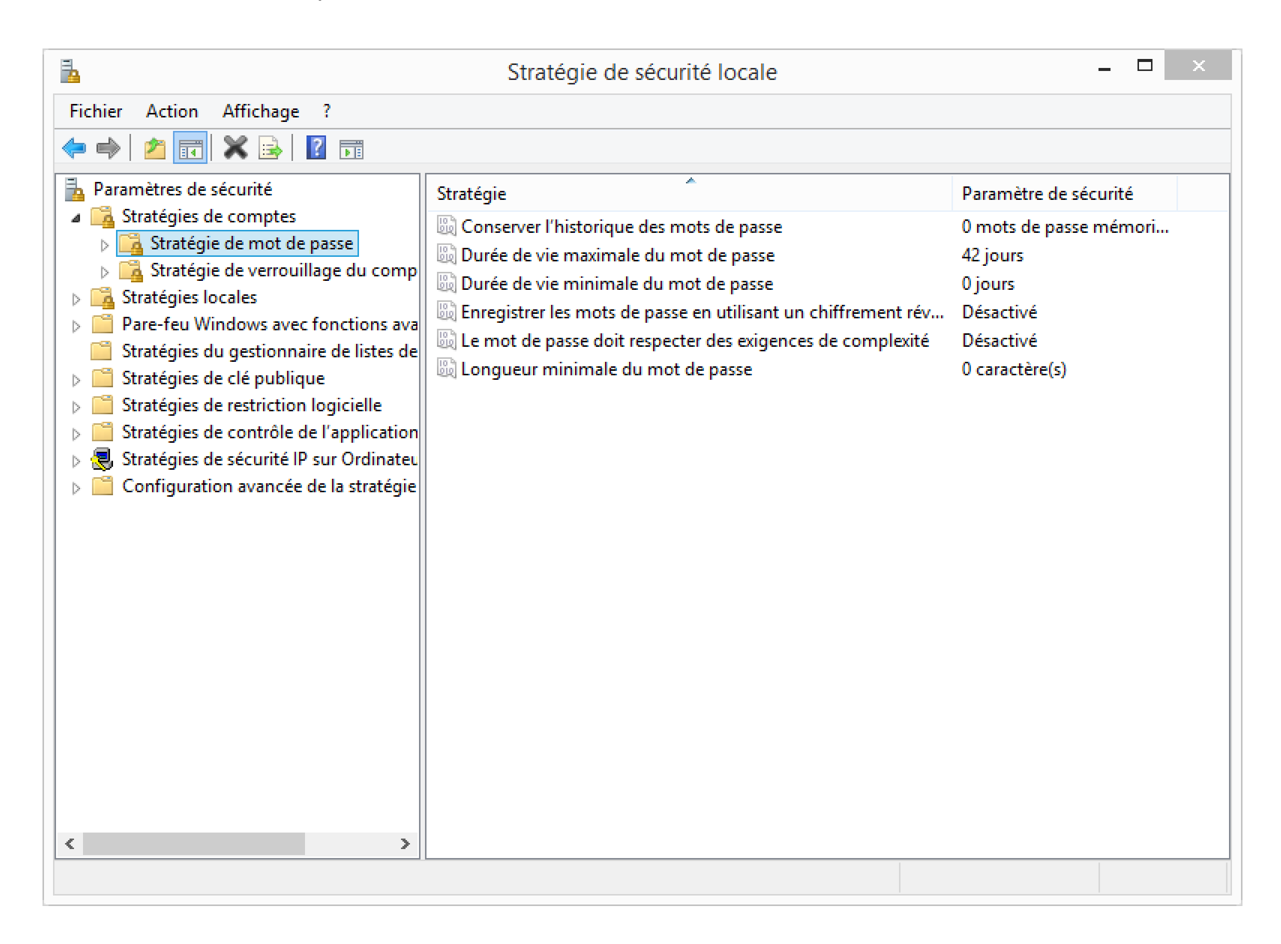
c. La fenêtre **Stratégie de sécurité locale** s'ouvre.



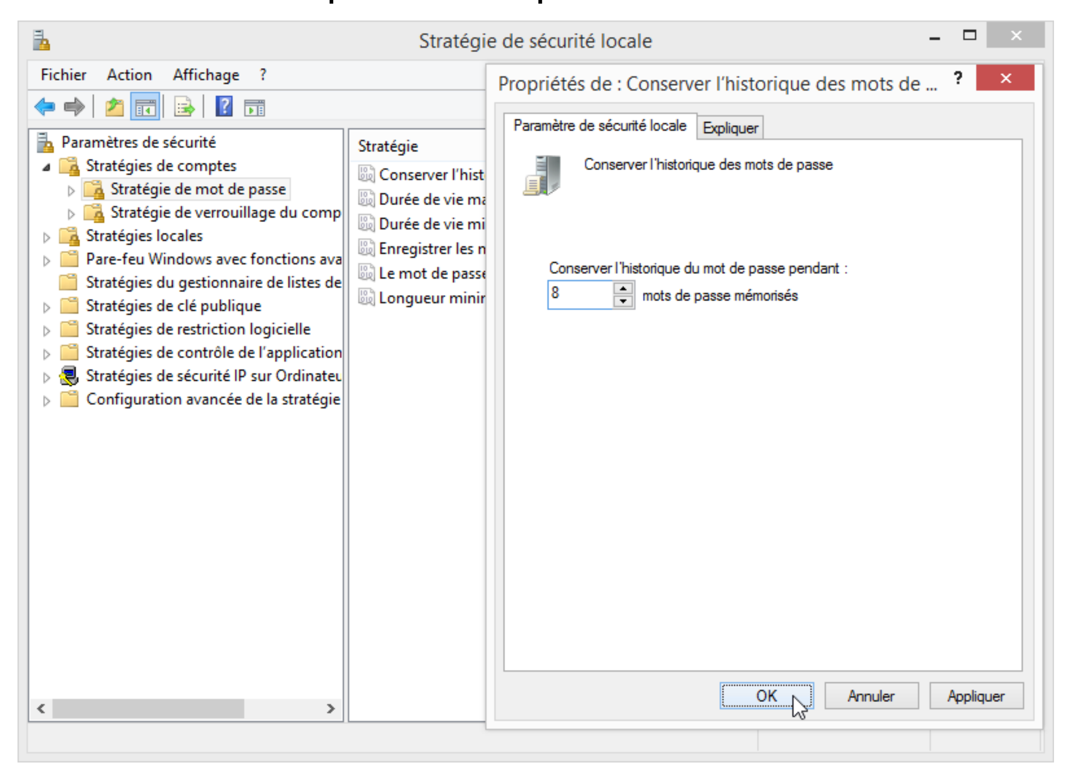
Étape 3 : Configurez les paramètres de sécurité Stratégie de mot de passe.

Les six premières exigences de la stratégie de sécurité de l'entreprise sont configurées dans la section **Stratégies de compte** de l'outil **Stratégie de sécurité locale**.

a. Cliquez sur la flèche en regard de **Stratégies de compte** pour développer cette section, puis cliquez sur **Stratégie de mot de passe**. Six stratégies sont affichées dans le panneau de droite avec les paramètres de sécurité associés par défaut.



b. La première stratégie, **Conserver l'historique des mots de passe**, est utilisée pour définir le nombre de mots de passe uniques que vous devez créer avant d'être autorisé à réutiliser un mot de passe. Selon la stratégie de sécurité de l'entreprise définie à l'étape 1, le paramètre de sécurité de cette stratégie doit être **8**. Double-cliquez sur **Conserver l'historique des mots de passe** pour ouvrir la fenêtre des propriétés **Conserver l'historique des mots de passe**. Définissez la valeur sur **8**.

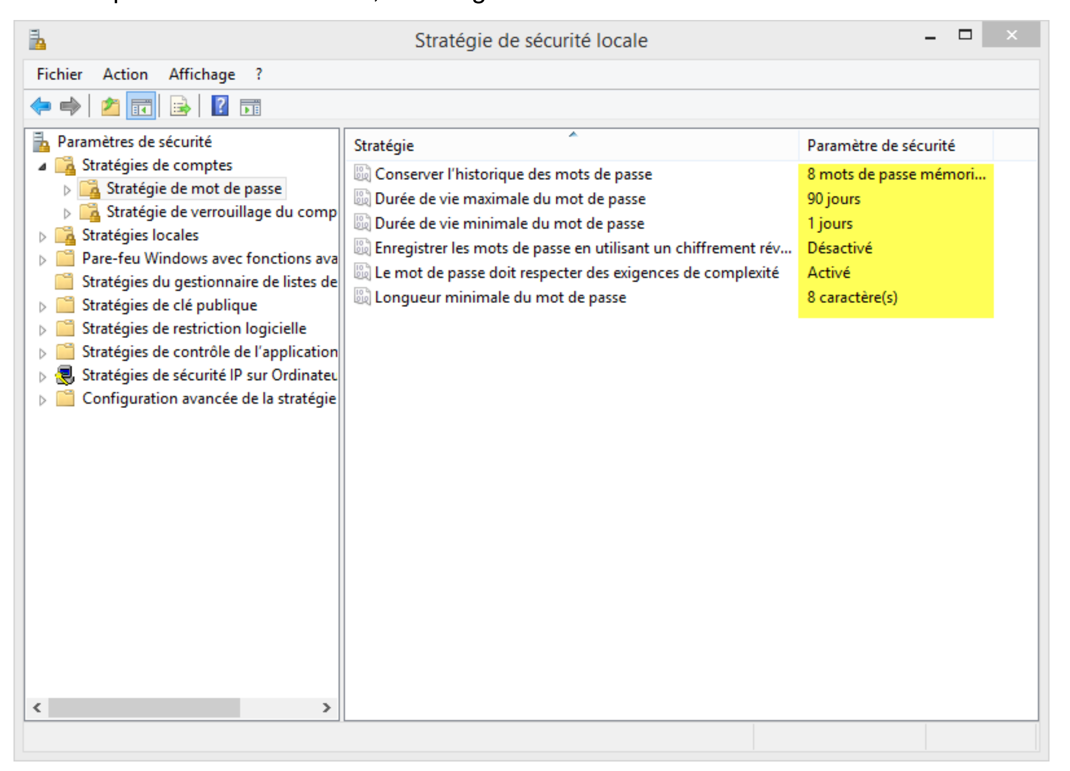


c. En vous basant sur les exigences de la stratégie de sécurité de l'étape 1, entrez les valeurs que vous devez définir dans **Stratégie de sécurité locale** pour les paramètres de sécurité restants de **Stratégie de mot de passe**.

Politique	Paramètre de sécurité
Appliquer l'historique des mots de passe	8
Durée de vie maximale du mot de passe	
Durée de vie minimale du mot de passe	
Longueur minimale du mot de passe	
Le mot de passe doit respecter des exigences de complexité	
Enregistrer les mots de passe en utilisant un chiffrement réversible	désactivé ;

Remarque : le paramètre de sécurité **Enregistrer les mots de passe en utilisant un chiffrement réversible** doit toujours être désactivé. Le fait d'enregistrer les mots de passe en utilisant un chiffrement réversible est pratiquement identique à l'enregistrement des mots de passe en clair. Pour cette raison, cette stratégie ne doit jamais être activée à moins que les besoins des applications soient plus importants que la nécessité de protéger les informations.

d. Double-cliquez sur chacune des stratégies et définissez les valeurs en fonction des entrées du tableau ci-dessus. Lorsque vous avez terminé, la configuration doit être similaire à celle-ci :

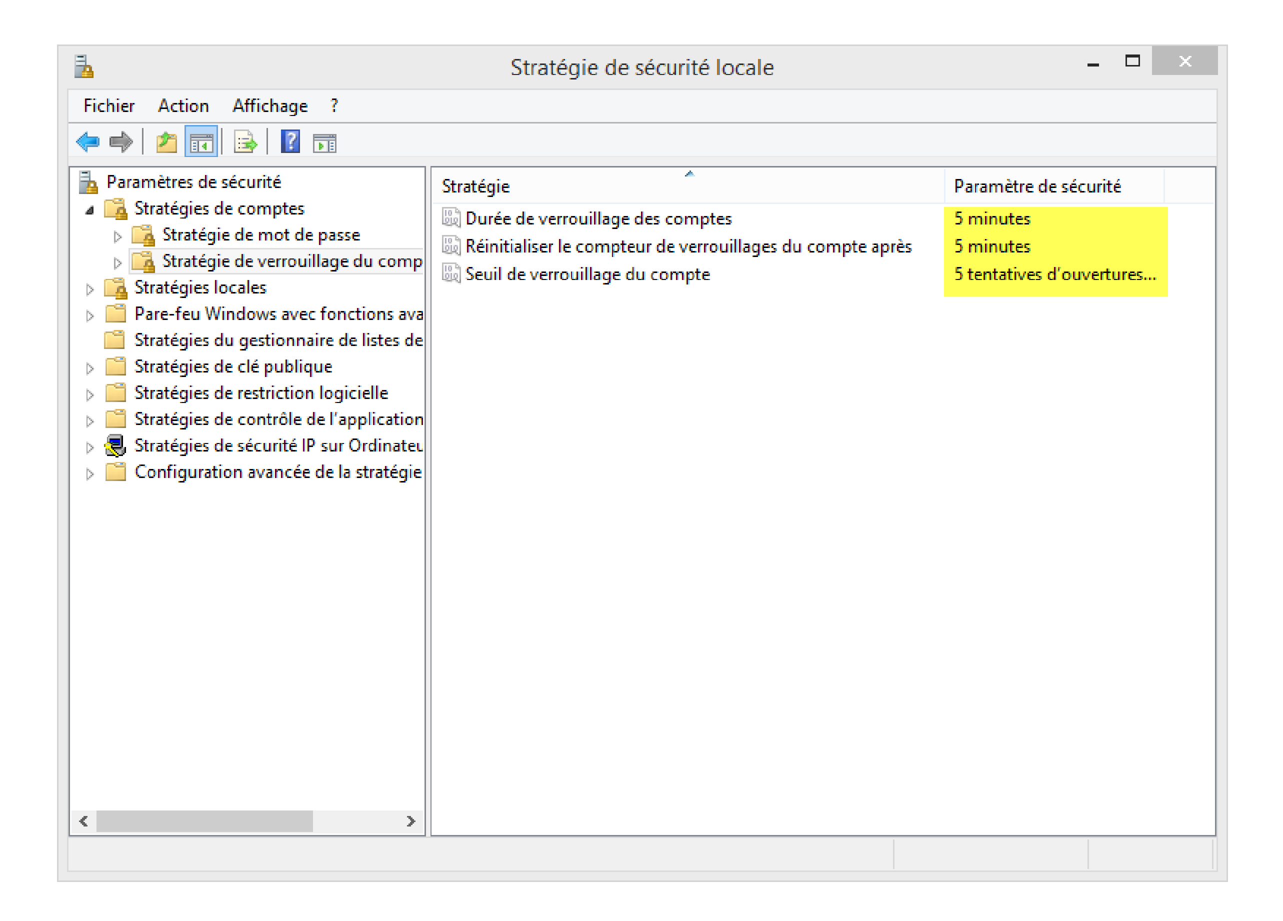


Étape 4 : Configurez les paramètres de sécurité Stratégie de verrouillage du compte.

a. Selon la stratégie de sécurité définie à l'étape 1, l'utilisateur est autorisé 5 tentatives d'ouvrir une session avant le verrouillage du compte.

b. L'utilisateur doit attendre 5 minute avant d'essayer de se reconnecter.

c. Utilisez les paramètres de sécurité **Stratégie de verrouillage du compte** dans **Stratégie de sécurité locale** pour configurer les exigences de la stratégie. Lorsque vous avez terminé, la configuration doit être similaire à celle-ci.
Conseil : vous devez d'abord configurer le **Seuil de verrouillage de compte**.

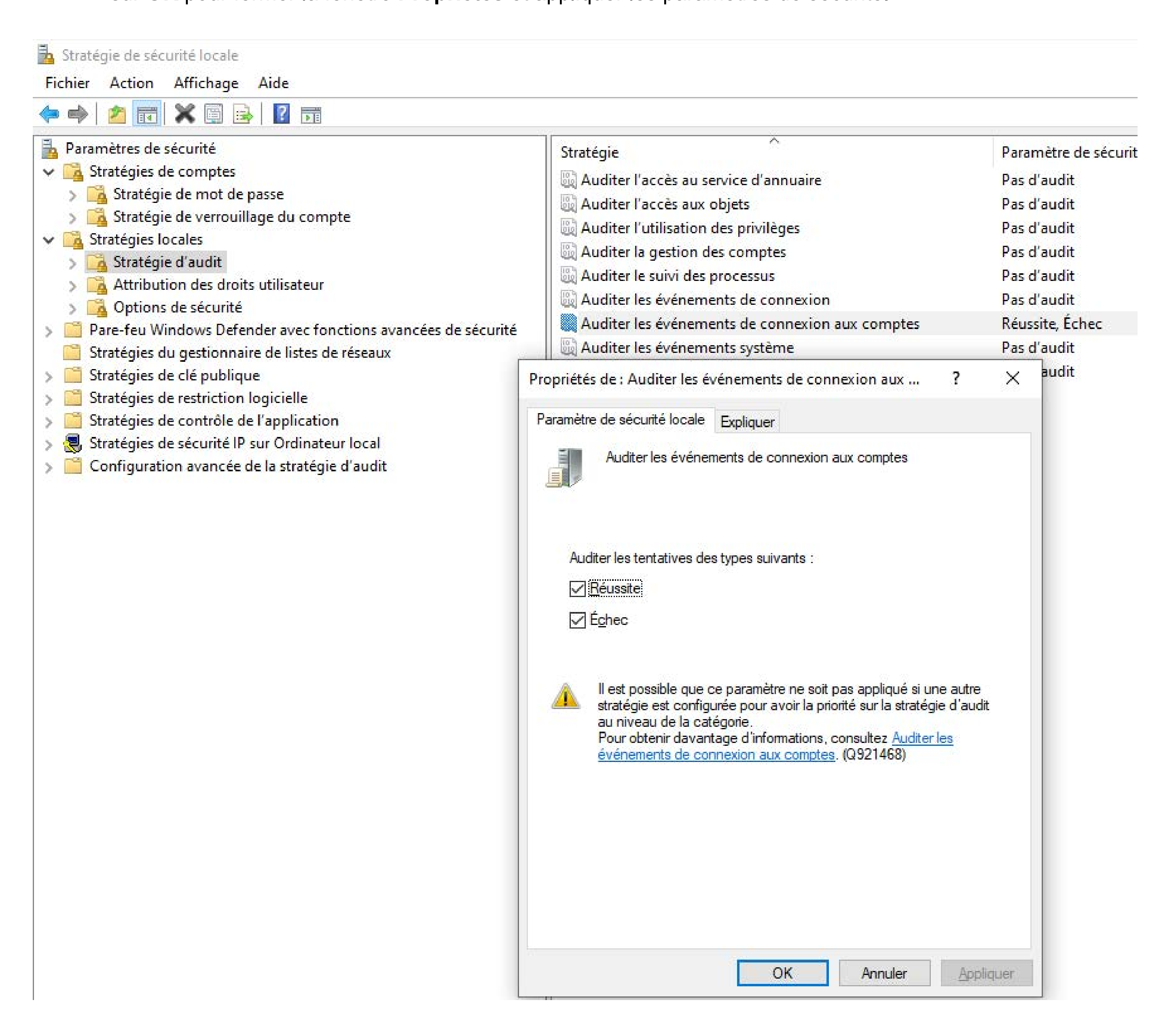


Étape 5 : Configurez les paramètres de sécurité de la stratégie d'audit.

a. Dans la **Stratégie de sécurité locale**, développez le menu **Stratégies locales**, puis cliquez sur **Stratégie d'audit**.

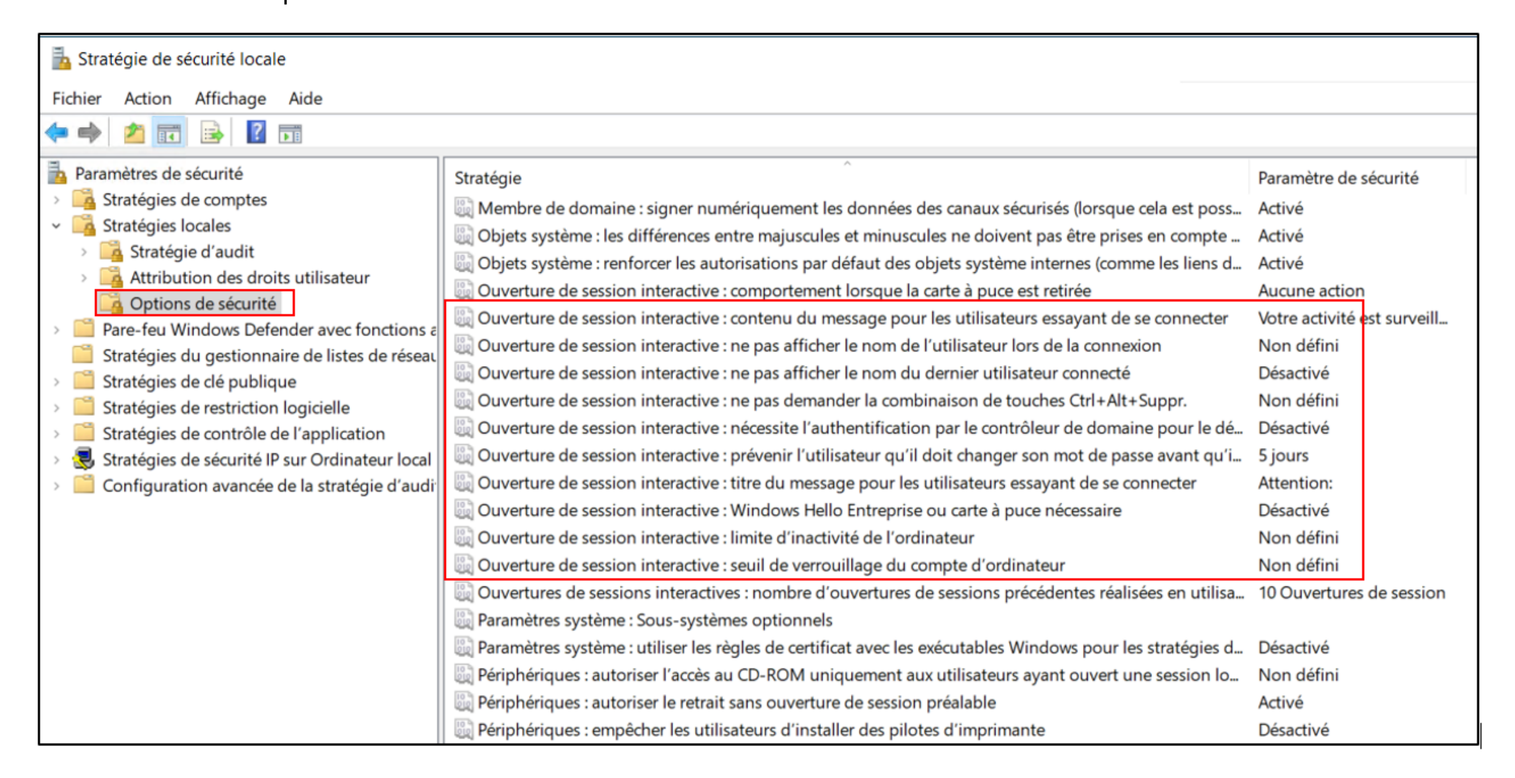
b. Double-cliquez sur **Auditer les événements de connexion aux comptes** pour ouvrir la fenêtre **Propriétés**. Cliquez sur l'onglet **Expliquer** pour en savoir plus sur ce paramètre de sécurité.

c. Cliquez sur l'onglet **Paramètre de sécurité**, puis activez les cases à cocher **Réussite** et **Échec**. Cliquez sur **OK** pour fermer la fenêtre **Propriétés** et appliquer les paramètres de sécurité.



Étape 6 : Configurez les paramètres de sécurité Stratégies locales.

a. Dans **Stratégie de sécurité locale**, cliquez sur **Options de sécurité** sous **Stratégies locales** pour afficher les paramètres de sécurité **Ouverture de session interactive.**.



b. À l'aide des **exigences de stratégie de sécurité restantes de l'étape 1 à la page 1**, dressez dans le tableau ci-dessous, la liste des stratégies et des paramètres de sécurité que vous devez modifier dans **Options de sécurité.**
La première stratégie est déjà indiquée pour vous. (Il y a trois autres paramètres à modifier):

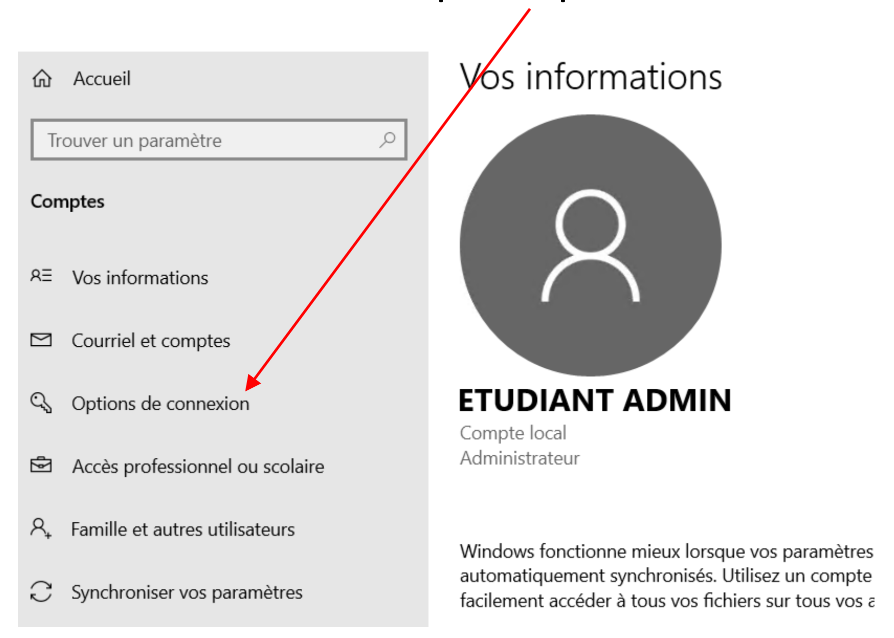
Politique	Paramètre de sécurité
Ouverture de session interactive : Limite d'inactivité de la machine	1800 secondes

c. Une fois que vous terminez de **configurer les 4 options**, fermez la fenêtre **Stratégie de sécurité locale.**

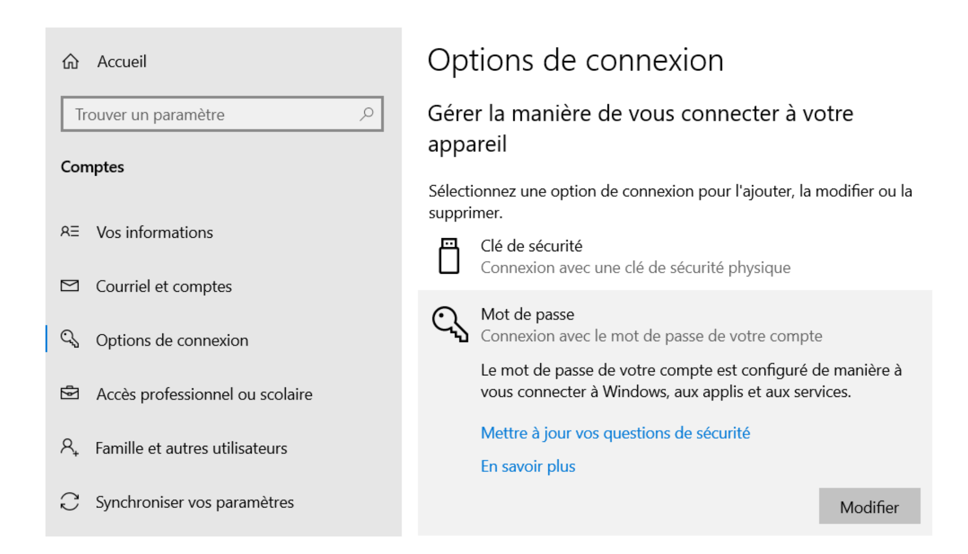
<u>Étape 7 : Testez les paramètres de sécurité Stratégie de mot de passe:</u>

Testez vos paramètres de sécurité Stratégie de mot de passe en essayant de changer le mot de passe. Essayez un nouveau mot de passe qui ne répond pas aux exigences de longueur ou de complexité. <u>Suivez ces étapes pour faire ce test:</u>

a. Ouvrez **Paramètres → Comptes → Options de connexion**



b. Sélectionnez **Mot de passe** puis **Modifier**



c. Entrez votre mot de passe actuel **420!winp4ss** puis cliquez sur **Suivant.**

d. Entrez ce nouveau mot de passe **123456** confirmez -le et entrez **test** dans le champ **Indication de mot de passe**

e. Cliquez sur **Suivant** puis **Terminer.**

f. Vous allez voir un message indiquant que **le nouveau mot de passe ne répond pas aux exigences de la stratégie de mot de passe.**

IMPORTANT 1: Prenez une capture d'écran de ce message et mettez-le dans le document Word.



g. Essayez encore une fois de modifier le mot de passe avec la suivante: **Passw0rd$**

h. Vous devez être capable de la modifier, car le nouveau mot de passe contient au **minimum 8 caractères** et **respecte les exigences de la complexité.**

Étape 8 : Testez les paramètres de sécurité Stratégie Options de sécurité :

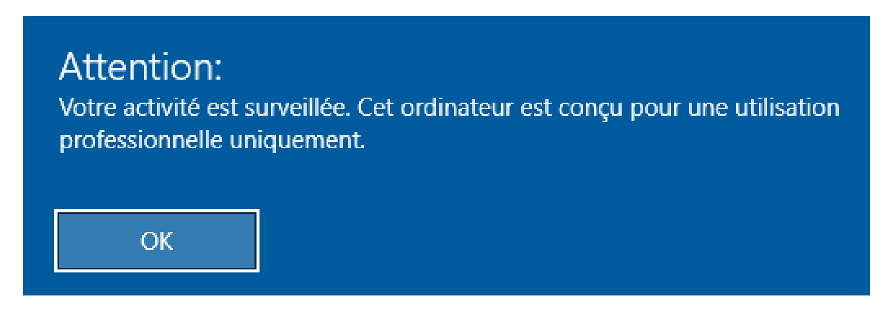
a. Déconnectez-vous de l'utilisateur **etudiantadmin**

b. Connectez-vous encore une fois avec **etudiantadmin** pour tester le nouveau mot de passe **Passw0rd$**

c. Si vous voyez ce message **Attention:**, donc votre nouvelle configuration des **Options de sécurité** de la **Stratégie locale** fonctionne très bien.

IMPORTANT 2: Prenez une capture d'écran de ce message et mettez-le dans le document Word.

d. Cliquez sur **OK** pour ouvrir la session.



Étape 9 : Testez les paramètres de sécurité Stratégie d'Audit :

a. Déconnectez-vous**.**

b. Connectez-vous encore une fois avec **etudiantadmin** et le mot de passe **123456.**

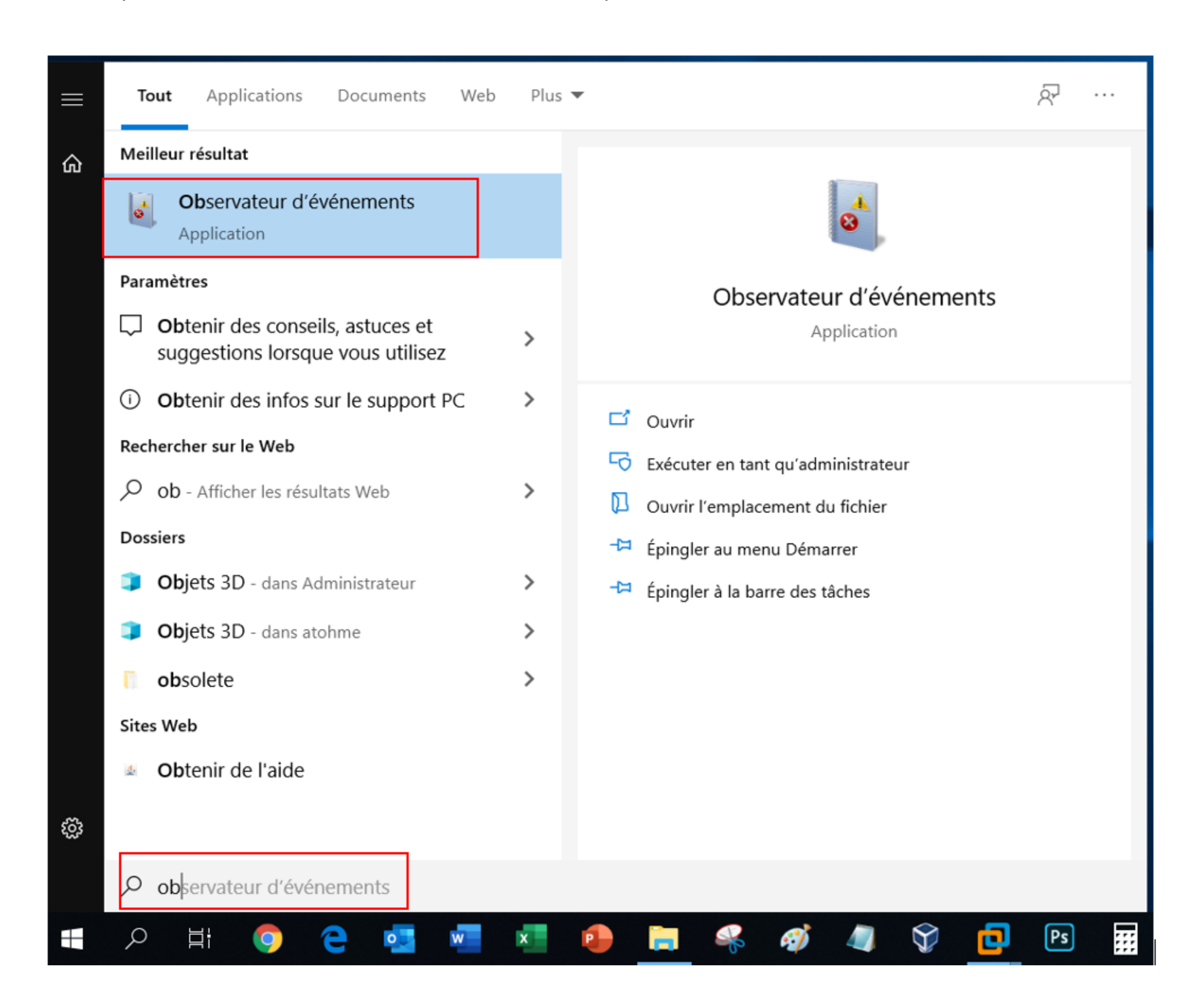
c. Vous allez avoir un message d'erreur que la tentative d'ouverture de session à échoué (sur Windows) et que ça n'a pas fonctionner, essayez encore une fois (sur les ordi MAC).

** Parce que vous avez tenté de se connecter **avec un mauvais mot de passe**, un **événement** est créé dans le **Journal de sécurité** de votre ordinateur.*

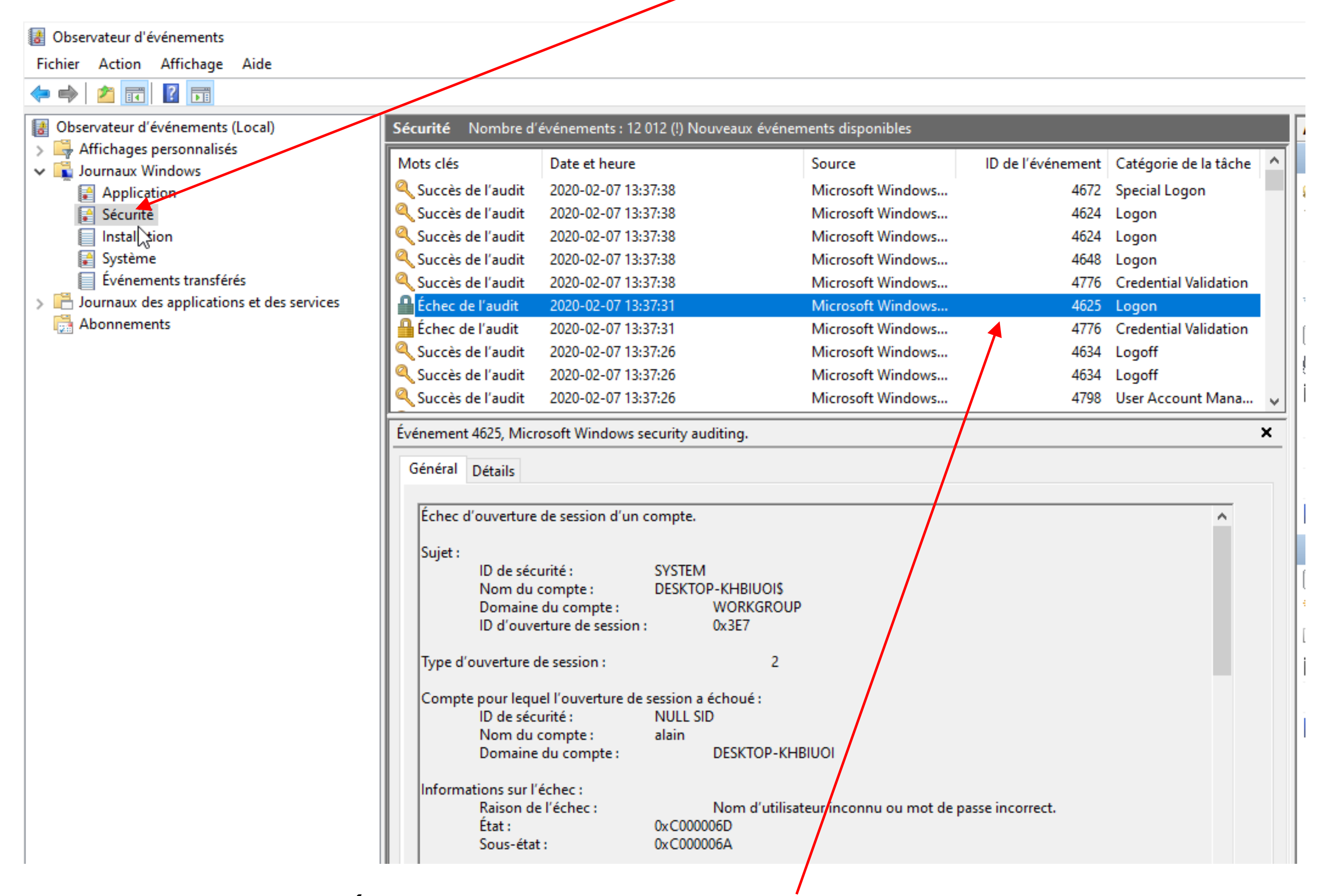
d. Tapez le bon mot de passe: **Passw0rd$** pour se connecter et aller vérifier le **Journal de sécurité.**

e. Pour accéder au **Journal de sécurité**, vous devez d'abord ouvrir l'outil **Observateur d'événements (Event viewer).**

f. Tapez **Observateur** dans le menu Windows pour ouvrir l'outil.



h. Dans **Observateur d'événements,** développez **Journaux Windows** puis sur **Sécurité** (pour ouvrir le **Journal de Sécurité**).



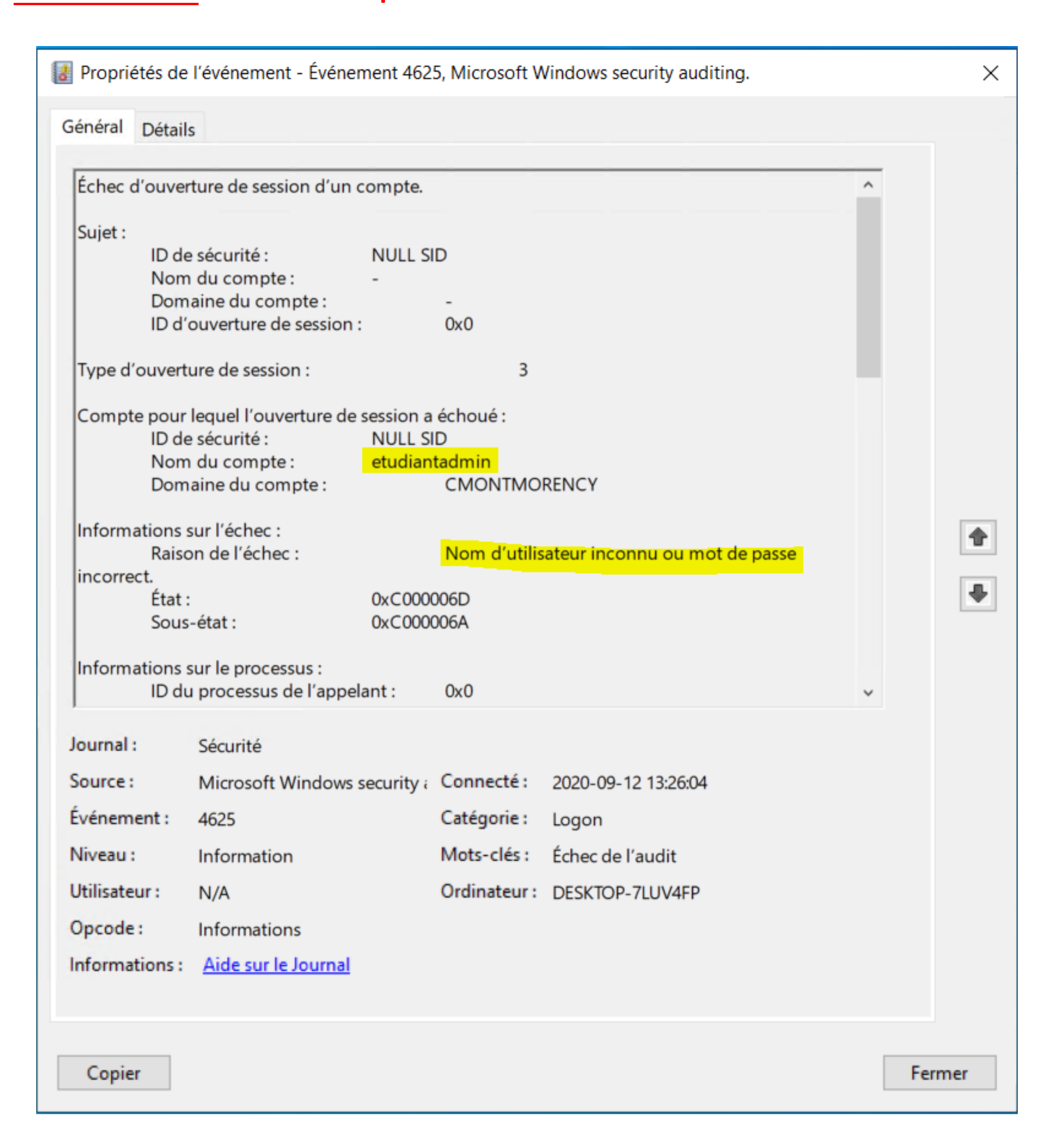
h. Cherchez l'événement **Échec de l'audit** avec l'ID **4625** et la catégorie de la tâche: **Logon.**

i. **Double-cliquez** sur l'événement pour l'ouvrir.

j. Cet événement été créé quand vous avez tentez d'ouvrir une session avec le **mauvais le mot de passe 123456**.

k. Observez les **Propriétés de cet évènement**.

IMPORTANT 3: Prenez une capture d'écran de cette fenêtre et mettez-le dans le document Word.



l. Une fois terminé, fermez l'**Observateur d'événements** et déconnectez-vous.